

The Cubic Case of Vinogradov's Mean Value Theorem — A Simplified Approach to Wooley's "Efficient Congruencing"

D.R. Heath-Brown
Mathematical Institute, Oxford

1 Introduction

In a remarkable series of papers, Wooley [3], [4], [5], [6], [7], and in collaboration with Ford [2], has made dramatic progress with Vinogradov's mean value theorem. This has culminated very recently in the full proof of the main conjecture, by Bourgain, Demeter and Guth [1], using rather different methods. Wooley's survey article [8] gives an excellent introduction to his results and their applications. The mean value theorem concerns the integer $J_{s,k}(X)$ defined as the number of solutions $(x_1, \dots, x_{2s}) \in \mathbb{N}^{2s}$ of the simultaneous equations

$$x_1^j + \dots + x_s^j = x_{s+1}^j + \dots + x_{2s}^j \quad (1 \leq j \leq k) \quad (1)$$

with $x_1, \dots, x_{2s} \leq X$. Here $X \geq 1$ is an arbitrary real number, and s and k are positive integers, which one treats as being fixed. The key feature of this system is that if (x_1, \dots, x_{2s}) is a solution, so is any translate $(x_1 + c, \dots, x_{2s} + c)$.

The various forms of the Vinogradov mean value theorem give upper bounds for $J_{s,k}(X)$. It is not hard to see that

$$J_{s,k}(X) \gg_{s,k} X^s + X^{2s-k(k+1)/2},$$

for $X \geq 1$, and the central conjecture is that

$$J_{s,k}(X) \ll_{s,k,\varepsilon} X^\varepsilon (X^s + X^{2s-k(k+1)/2})$$

for any $\varepsilon > 0$. "Classically" this was known for $k = 1$ and 2 , for $s \leq k + 1$, and for $s \geq s_0(k)$ with a value $s_0(k) \ll k^2 \log k$. However Wooley [6] shows that one may take $s_0(k) = k^2 - k + 1$, and that the conjecture also holds for $s \leq s_1(k)$ with $s_1(k) = k(k+1)/2 - k/3 + o(k)$. Finally, in [7], he shows that the conjecture holds for $k = 3$.

The purpose of this paper is to present a much simplified version of Wooley's methods, sufficient to handle the case $k = 3$.

Theorem *We have*

$$J_{6,3}(X) \ll_\varepsilon X^{3+\varepsilon}$$

for any fixed $\varepsilon > 0$.

It is trivial from (2) below that if s and t are any positive integers then we will have $J_{s+t,k}(X) \leq X^{2t} J_{s,k}(X)$ and $J_{s,k}(X) \leq J_{s+t,k}(X)^{s/(s+t)}$. Thus for $k = 3$ we can deduce the general case of the conjecture immediately from the theorem.

It should be stressed that, while the argument of the present paper appears cleaner than that presented by Wooley [7], it is merely a simplification of his version. The underlying principles are the same. It is not a “different” proof. In part the simplification arises from the restriction to the case $k = 3$.

2 Outline of the Proof

Investigations into the mean value theorem depend crucially on an alternative interpretation of $J_{s,k}(X)$ in terms of exponential sums. If $\alpha \in \mathbb{R}^k$ we write

$$f_k(\alpha; X) = f(\alpha) = \sum_{x \leq X} e(\alpha_1 x + \dots + \alpha_k x^k),$$

whence

$$J_{s,k}(X) = \int_{(0,1]^k} |f(\alpha)|^{2s} d\alpha. \quad (2)$$

Our version of the efficient congruencing method will also use the exponential sums

$$f_k(\alpha; X, \xi, a) = f_a(\alpha; \xi) = \sum_{\substack{x \leq X \\ x \equiv \xi \pmod{p^a}}} e(\alpha_1 x + \dots + \alpha_k x^k),$$

where p is prime and a is a positive integer exponent. The prime $p \geq 5$ will be fixed throughout the argument, so we will not include it explicitly among the parameters for $f_a(\alpha; \xi)$. Taking s and k as fixed we will write

$$I_m(X; \xi, \eta; a, b) = \int_{(0,1]^k} |f_a(\alpha; \xi)|^{2m} |f_b(\alpha; \eta)|^{2(s-m)} d\alpha, \quad (0 \leq m \leq s-1),$$

which counts solutions of (1) in which

$$x_i \equiv \xi \pmod{p^a} \quad (1 \leq i \leq m \text{ and } s+1 \leq i \leq s+m),$$

and

$$x_i \equiv \eta \pmod{p^b} \quad (m+1 \leq i \leq s \text{ and } s+m+1 \leq i \leq 2s).$$

The reader should think of this as a simplified version of Wooley’s $I_{a,b}^{m,r}(X; \xi, \eta)$, given by [6, (2.11)]. We observe that when $m = 0$ we have

$$I_0(X; \xi, \eta; a, b) = \int_{(0,1]^k} |f_b(\alpha; \eta)|^{2s} d\alpha,$$

which is independent of ξ and a .

We will also work with $I_m(X; a, b)$ defined by

$$I_0(X; a, b) = \max_{\eta \pmod{p}} I_0(X; \xi, \eta; a, b)$$

and

$$I_m(X; a, b) = \max_{\xi \not\equiv \eta \pmod{p}} I_m(X; \xi, \eta; a, b) \quad (1 \leq m \leq s-1).$$

The condition $\xi \not\equiv \eta \pmod{p}$ is the last remaining vestige of Wooley's "conditioning" step. We note for future reference the trivial symmetry relation

$$I_m(X; a, b) = I_{s-m}(X; b, a).$$

Although many of our results can be proved for general s and k we shall now specialize to the case $s = 6$, $k = 3$, and write $J(X) = J_{6,3}(X)$ for brevity. When $m = 0$ we can relate $I_0(X; a, b)$ to J as follows.

Lemma 1 *If $p^b \leq X$ we have*

$$I_0(X; a, b) \leq J(2X/p^b).$$

We will prove this in the next section along with a number of other estimates relating different values of $I_1(X; a, b)$ and $I_2(X; a, b)$. Our next result shows how to bound $J(X)$ in terms of $I_2(X; 1, 1)$.

Lemma 2 *If $p \leq X$ we have*

$$J(X) \ll pJ(2X/p) + p^{12}I_2(X; 1, 1).$$

One way to compare values of $I_1(X; a, b)$ and $I_2(X; a, b)$ is by applying Hölder's inequality. We give two such estimates.

Lemma 3 *We have*

$$I_2(X; a, b) \leq I_2(X; b, a)^{1/3} I_1(X; a, b)^{2/3}.$$

Lemma 4 *If $p^b \leq X$ we have*

$$I_1(X; a, b) \leq I_2(X; b, a)^{1/4} J(2X/p^b)^{3/4}.$$

Next we show how successively larger values of a and b arise.

Lemma 5 *We have*

$$I_1(X; a, b) \leq p^{3b-a} I_1(X; 3b, b)$$

if $1 \leq a \leq 3b$.

Finally we shall need a result analogous to Lemma 5 for $I_2(X; a, b)$.

Lemma 6 . *If $1 \leq a \leq b$ we have*

$$I_2(X; a, b) \leq 2bp^{4(b-a)} I_2(X; 2b-a, b).$$

We are now ready to assemble all these results to prove the following recursive estimate.

Lemma 7 *If $1 \leq a \leq b$ and $p^b \leq X$ we have*

$$I_2(X; a, b) \leq 2bp^{-10a/3+14b/3} I_2(X; b, 2b-a)^{1/3} I_2(X; b, 3b)^{1/6} J(2X/p^b)^{1/2}.$$

For the proof we successively apply Lemmas 6, 3, 5 and 4, giving

$$\begin{aligned}
I_2(X; a, b) &\leq 2bp^{4(b-a)}I_2(X; 2b-a, b) \\
&\leq 2bp^{4(b-a)}I_2(X; b, 2b-a)^{1/3}I_1(X; 2b-a, b)^{2/3} \\
&\leq 2bp^{4(b-a)}I_2(X; b, 2b-a)^{1/3}\left\{p^{3b-(2b-a)}I_1(X; 3b, b)\right\}^{2/3} \\
&\leq 2bp^{4(b-a)+2(a+b)/3}I_2(X; b, 2b-a)^{1/3} \\
&\quad \times \left\{I_2(X; b, 3b)^{1/4}J(2X/p^b)^{3/4}\right\}^{2/3} \\
&= 2bp^{-10a/3+14b/3}I_2(X; b, 2b-a)^{1/3}I_2(X; b, 3b)^{1/6}J(2X/p^b)^{1/2}.
\end{aligned}$$

Here we should observe that, in applying Lemma 5 to $I_1(X; 2b-a, b)$ the necessary condition “ $a \leq 3b$ ” is satisfied, since $2b-a \leq 3b$.

Everything is now in place to complete the proof of the theorem. We note the trivial upper bound $J(X) \ll X^{12}$ and the trivial lower bound $J(X) \geq [X]^6 \gg X^6$ (coming from the obvious diagonal solutions $x_i = x_{6+i}$ for $i \leq 6$). Thus we may define a real number $\Delta \in [0, 6]$ by setting

$$\Delta = \inf\{\delta \in \mathbb{R} : J(X) \ll X^{6+\delta} \text{ for } X \geq 1\}. \quad (3)$$

It follows that we will have $J(X) \ll_\varepsilon X^{6+\Delta+\varepsilon}$ for any $\varepsilon > 0$. Our goal of course is to show that $\Delta = 0$.

We observe that

$$I_2(X; a, b) \leq J(X) \ll_\varepsilon X^{6+\Delta+\varepsilon}$$

for $1 \leq a \leq b$, and hence that

$$I_2(X; a, b) \ll_\varepsilon X^{6+\Delta+\varepsilon}p^{-2a-4b}p^{3(3b-a)}, \quad (4)$$

since $3(3b-a) \geq 2a+4b$ for $a \leq b$. We now proceed to use Lemma 7 to prove, by induction on n , that

$$I_2(X; a, b) \ll_{\varepsilon, n, a, b} X^{6+\Delta+\varepsilon}p^{-2a-4b}p^{(3-n\Delta/6)(3b-a)} \quad (5)$$

for any integer $n \geq 0$, provided that

$$1 \leq a \leq b \quad (6)$$

and

$$p^{3^n b} \leq X. \quad (7)$$

The base case $n = 0$ is exactly the bound (4). The reader may be puzzled by the choice of the exponent for p in (5). We shall discuss this further in the final section.

Given (5) we have

$$\begin{aligned}
I_2(X; b, 2b-a) &\ll_{\varepsilon, n, a, b} X^{6+\Delta+\varepsilon}p^{-2b-4(2b-a)}p^{(3-n\Delta/6)(3(2b-a)-b)} \\
&= X^{6+\Delta+\varepsilon}p^{4a-10b}p^{(3-n\Delta/6)(5b-3a)}.
\end{aligned}$$

Note that the conditions corresponding to (6) and (7) are satisfied if

$$p^{3^{n+1}b} \leq X.$$

since we will have $1 \leq b \leq 2b - a$ whenever $1 \leq a \leq b$, and

$$p^{3^n(2b-a)} \leq p^{3^{n+1}b} \leq X.$$

In a similar way, (5) implies that

$$\begin{aligned} I_2(X; b, 3b) &\ll_{\varepsilon, n, b} X^{6+\Delta+\varepsilon} p^{-2b-12b} p^{(3-n\Delta/6)(9b-b)} \\ &= X^{6+\Delta+\varepsilon} p^{-14b} p^{(3-n\Delta/6)(8b)} \end{aligned}$$

the conditions corresponding to (6) and (7) holding whenever $b \geq 1$.

Finally we have

$$J(2X/p^b) \ll_{\varepsilon} X^{6+\Delta+\varepsilon} p^{-6b-\Delta b}$$

provided that $p^b \leq X$. Feeding these estimates into Lemma 7 we deduce that

$$\begin{aligned} I_2(X; a, b) &\ll_{\varepsilon, n, a, b} p^{-10a/3+14b/3} \{X^{6+\Delta+\varepsilon} p^{4a-10b} p^{(3-n\Delta/6)(5b-3a)}\}^{1/3} \\ &\quad \times \{X^{6+\Delta+\varepsilon} p^{-14b} p^{(3-n\Delta/6)(8b)}\}^{1/6} \{X^{6+\Delta+\varepsilon} p^{-6b-\Delta b}\}^{1/2} \\ &= X^{6+\Delta+\varepsilon} p^{-2a-4b} p^{(3-n\Delta/6)(3b-a)} p^{-\Delta b/2} \\ &\leq X^{6+\Delta+\varepsilon} p^{-2a-4b} p^{(3-(n+1)\Delta/6)(3b-a)}, \end{aligned}$$

since $b/2 \geq (3b-a)/6$. This provides the required induction step.

Having established (5) we apply it with $a = b = 1$, and p chosen to lie in the range

$$\frac{1}{2} X^{1/3^n} \leq p \leq X^{1/3^n}.$$

There will always be a suitable $p \geq 5$ if

$$X \geq 10^{3^n}.$$

We then deduce from Lemma 2 that

$$J(X) \ll pJ(2X/p) + p^{12} I_2(X; 1, 1) \ll_{\varepsilon, n} p(X/p)^{6+\Delta+\varepsilon} + X^{6+\Delta+\varepsilon} p^{12-n\Delta/3}.$$

If Δ were strictly positive we could choose n sufficiently large that $n\Delta \geq 39$, and would then conclude that

$$J(X) \ll_{\varepsilon, n} X^{6+\Delta+\varepsilon} p^{-1} \ll_{\varepsilon, n} X^{6+\Delta-3^{-n}+\varepsilon},$$

contradicting the definition (3). We must therefore have $\Delta = 0$, as required for the theorem.

The reader will probably feel that the final stages of the argument, from (5) onward, are lacking in motivation. The final section of the paper will offer an explanation for the route chosen.

3 Proof of the Lemmas

We begin by examining Lemma 1. We observe that there is an $\eta \in (0, p^b]$ such that $I_0(X; a, b)$ counts solutions to (1) in which each x_i takes the shape $\eta + p^b y_i$, with integer variables y_i . We will have $0 \leq y_i \leq X/p^b$. Thus if we set $z_i = y_i + 1$ we find that $1 \leq z_i \leq 1 + X/p^b \leq 2X/p^b$, in view of our condition $p^b \leq X$. Moreover we know that if the x_i satisfy (1) then so will the y_i and the z_i . It follows that $I_0(X; a, b) \leq J_{s,k}(2X/p^b)$ as claimed.

To prove Lemma 2 we split solutions of (1) into congruence classes for which $x_i \equiv \xi_i \pmod{p}$ for $1 \leq i \leq 12$. The number of solutions in which

$$x_1 \equiv \dots \equiv x_{12} \pmod{p}$$

is at most

$$\sum_{\eta \pmod{p}} I_0(X; 0, \eta; 1, 1) \leq p I_0(X; 1, 1) \leq p J(2X/p),$$

by Lemma 1. For the remaining solutions to (1) there is always a pair of variables that are incongruent modulo p , and it follows that there exist $\xi \not\equiv \eta \pmod{p}$ such that

$$J(X) \leq p J(2X/p) + \binom{12}{2} p(p-1) \int_{(0,1]^3} |f_1(\alpha; \xi_i) f_1(\alpha; \mu) f(\alpha)^{10}| d\alpha.$$

By Hölder's inequality we have

$$\begin{aligned} & \int_{(0,1]^3} |f_1(\alpha; \xi_i) f_1(\alpha; \mu) f(\alpha)^{10}| d\alpha \\ & \leq \left\{ \int_{(0,1]^3} |f_1(\alpha; \xi_i)|^4 |f_1(\alpha; \mu)|^8 d\alpha \right\}^{1/12} \\ & \quad \times \left\{ \int_{(0,1]^3} |f_1(\alpha; \xi_i)|^8 |f_1(\alpha; \mu)|^4 d\alpha \right\}^{1/12} \\ & \quad \times \left\{ \int_{(0,1]^3} |f(\alpha)|^{2s} d\alpha \right\}^{5/6}, \end{aligned}$$

whence

$$J(X) \ll p J(2X/p) + p^2 I_2(X; 1, 1)^{1/12} I_2(X; 1, 1)^{1/12} J(X)^{5/6}.$$

We deduce that

$$J(X) \ll p J(2X/p) + p^{12} I_2(X; 1, 1),$$

as required for the lemma.

Lemma 3 is a trivial application of Holder's inequality. We have

$$\begin{aligned} I_2(X; \xi, \eta; a, b) &= \int_{(0,1]^3} |f_a(\alpha; \xi)|^4 |f_b(\alpha; \eta)|^8 d\alpha \\ &\leq \left\{ \int_{(0,1]^3} |f_a(\alpha; \xi)|^8 |f_b(\alpha; \eta)|^4 d\alpha \right\}^{1/3} \\ &\quad \times \left\{ \int_{(0,1]^3} |f_a(\alpha; \xi)|^2 |f_b(\alpha; \eta)|^{10} d\alpha \right\}^{2/3} \\ &\leq I_2(X; b, a)^{1/3} I_1(X; a, b)^{2/3} \\ &= I_1(X; a, a), \end{aligned}$$

and the lemma follows.

For Lemma 4 we note that

$$\begin{aligned}
I_1(X; \xi, \eta; a, b) &= \int_{(0,1]^3} |f_a(\alpha; \xi)|^2 |f_b(\alpha; \eta)|^{10} d\alpha \\
&\leq \left\{ \int_{(0,1]^3} |f_b(\alpha; \xi)|^4 |f_a(\alpha; \eta)|^8 d\alpha \right\}^{1/4} \\
&\quad \times \left\{ \int_{(0,1]^3} |f_b(\alpha; \eta)|^{12} d\alpha \right\}^{3/4} \\
&\leq I_2(X; b, a)^{1/4} I_0(X; b, b)^{3/4} \\
&\leq I_2(X; b, a)^{1/4} J(2X/p^b)^{3/4},
\end{aligned}$$

by Hölder's inequality and Lemma 1.

Turning next to Lemma 5 we note that $I_1(X; \xi, \eta; a, b)$ counts solutions of (1) in which $x_i = \xi + p^a y_i$ for $i = 1$ and $i = 7$, and $x_i = \eta + p^b y_i$ for the remaining indices i . If we set $\nu = \xi - \eta$ we deduce that the variables

$$z_i = \begin{cases} \nu + p^a y_i, & i = 1 \text{ or } 7, \\ p^b y_i, & \text{otherwise,} \end{cases}$$

also satisfy (1). In particular, the equation of degree $j = 3$ yields

$$(\nu + p^a z_1)^3 \equiv (\nu + p^a z_7)^3 \pmod{p^{3b}}.$$

Now, crucially, we use the fact that $\xi \not\equiv \eta \pmod{p}$, whence $p \nmid \nu$. It follows that we must have $\nu + p^a z_1 \equiv \nu + p^a z_{s+1} \pmod{p^{3b}}$, and hence $z_1 \equiv z_{s+1} \pmod{p^{3b-a}}$. We therefore have $x_1 \equiv x_7 \equiv \xi' \pmod{p^{3b}}$ for one of p^{3b-a} possible values of ξ' , so that

$$I_1(X; \xi, \eta; a, b) \leq p^{3b-a} I_1(X; 3b, b),$$

which suffices for the lemma.

Finally we must handle Lemma 6. We note that $I_2(X; \xi, \eta; a, b)$ counts solutions of (1) in which $x_i = \xi + p^a y_i$ for $i = 1, 2, 7$ and 8 , and $x_i = \eta + p^b y_i$ for the remaining indices i . As in the proof of Lemma 5 we set $\nu = \xi - \eta$ and $z_i = x_i - \eta$, so that the z_i also satisfy (1). We will have $p^b \mid z_i$ for $3 \leq i \leq 6$ and $9 \leq i \leq 12$, whence

$$(\nu + p^a y_1)^j + (\nu + p^a y_2)^j \equiv (\nu + p^a y_7)^j + (\nu + p^a y_8)^j \pmod{p^{bj}} \quad (1 \leq j \leq 3)$$

with $\nu = \xi - \eta \not\equiv 0 \pmod{p}$. We shall use only the congruences for $j = 2$ and 3 . On expanding these we find that

$$2\nu S_1 + p^a S_2 \equiv 0 \pmod{p^{2b-a}} \tag{8}$$

and

$$3\nu^2 S_1 + 3\nu p^a S_2 + p^{2a} S_3 \equiv 0 \pmod{p^{3b-a}},$$

where

$$S_j = y_1^j + y_2^j - y_7^j - y_8^j \quad (j = 1, 2, 3).$$

Eliminating S_1 from these yields

$$3\nu p^a S_2 + 2p^{2a} S_3 \equiv 0 \pmod{p^{2b-a}},$$

whence

$$3\nu S_2 + 2p^a S_3 \equiv 0 \pmod{p^{2b-2a}}.$$

Moreover (8) trivially implies that

$$2\nu S_1 + p^a S_2 \equiv 0 \pmod{p^{2b-2a}}.$$

It appears that we have wasted some information here, but that turns out not to be the case.

We now call on the following result, which we shall prove at the end of this section.

Lemma 8 *With the notations above for S_j , let $N(p; a, c)$ denote the number of solutions (y_1, y_2, y_7, y_8) modulo p^c of the congruences*

$$2\nu S_1 + p^a S_2 \equiv 3\nu S_2 + 2p^a S_3 \equiv 0 \pmod{p^c}.$$

Then if $a \geq 1$ and $c \geq 0$ we will have $N(p; a, c) \leq (c+1)p^{2c}$.

If $y_i \equiv y_{i0} \pmod{p^{2(b-a)}}$ for $i = 1, 2, 7, 8$ then $x_i \equiv \xi_i \pmod{p^{2b-a}}$, with $\xi_i = \xi + p^a y_{i0}$. The number of solutions to (1) counted by $I_2(X; \xi, \eta; a, b)$ for which $y_i \equiv y_{i0} \pmod{p^{2(b-a)}}$ is then given by

$$\begin{aligned} & \int_{(0,1]^3} f_{2b-a}(\alpha; \xi_1) f_{2b-a}(\alpha; \xi_2) \overline{f_{2b-a}(\alpha; \xi_7) f_{2b-a}(\alpha; \xi_8)} |f_b(\alpha; \eta)|^8 d\alpha \\ & \leq \int_{(0,1]^3} \left| \prod_{i=1,2,6,7} f_{2b-a}(\alpha; \xi_i) \right| |f_b(\alpha; \eta)|^8 d\alpha \\ & \leq \prod_{i=1,2,6,7} \left\{ \int_{(0,1]^3} |f_{2b-a}(\alpha; \xi_i)|^4 |f_b(\alpha; \eta)|^8 d\alpha \right\}^{1/4} \\ & \leq \prod_{i=1,2,6,7} I_2(X; \xi_i, \eta; 2b-a, a)^{1/4} \\ & \leq I_2(X; 2b-a, a), \end{aligned}$$

by Holder's inequality. It then follows from Lemma 8 that

$$I_2(X; a, b) \leq N(p; a, 2(b-a)) I_2(X; 2b-a, b) \leq 2bp^{4(b-a)} I_2(X; 2b-a, a)$$

as required.

It remains to prove Lemma 8, for which we use induction on c . The base case $c = 0$ is trivial. When $c = 1$ we have $p \mid S_1$ and $p \mid S_2$ and the number of solutions is $2p^2 - p$, which is also satisfactory. In general we shall say that a solution (y_1, y_2, y_7, y_8) is singular if

$$y_1 \equiv y_2 \equiv y_7 \equiv y_8 \pmod{p},$$

and nonsingular otherwise. For a nonsingular solution the vectors

$$\nabla(2\nu S_1 + p^a S_2) \quad \text{and} \quad \nabla(3\nu S_2 + 2p^a S_3)$$

are not proportional modulo p , since $a \geq 1$ and $p \nmid 6\nu$. It follows that a nonsingular solution (y_1, y_2, y_7, y_8) of the congruences modulo p^c will lift to

exactly p^2 solutions modulo p^{c+1} . Thus if we write $N_0(p; a, c)$ for the number of nonsingular solutions modulo p^c we will have $N_0(p; a, c) \leq 2p^{2c}$, by induction.

For a singular solution we have

$$y_1 \equiv y_2 \equiv y_7 \equiv y_8 \equiv \beta \pmod{p},$$

say. If we write $y_i = \beta + pu_i$ and

$$S'_j = u_1^j + u_2^j - u_7^j - u_8^j$$

we find that

$$2\nu S_1 + p^a S_2 = 2(\nu + \beta p^a) p S'_1 + p^{a+2} S'_2$$

and

$$3\nu S_2 + 2p^a S_3 = 6\beta(\nu + \beta p^a) p S'_1 + 3(\nu + 2\beta p^a) p^2 S'_2 + 2p^{a+3} S'_3.$$

Hence

$$2\nu' p S'_1 + p^{a+2} S'_2 \equiv 6\beta \nu' p S'_1 + 3(\nu' + \beta p^a) p^2 S'_2 + 2p^{a+3} S'_3 \equiv 0 \pmod{p^c}$$

with $\nu' = \nu + \beta p^a \not\equiv 0 \pmod{p}$. Eliminating S'_1 from the second expression yields

$$3\nu' p^2 S'_2 + 2p^{3+a} S'_3 \equiv 0 \pmod{p^c}$$

and we deduce that

$$2\nu' S'_1 + p^{a+1} S'_2 \equiv 0 \pmod{p^{c-1}} \tag{9}$$

and

$$3\nu' S'_2 + 2p^{a+1} S'_3 \equiv 0 \pmod{p^{c-2}}. \tag{10}$$

Since we are counting values of y_i modulo p^c we have to count values of u_i modulo p^{c-1} . However any solution of

$$2\nu' S'_1 + p^{a+1} S'_2 \equiv 3\nu' S'_2 + 2p^{a+1} S'_3 \equiv 0 \pmod{p^{c-2}}$$

modulo p^{c-2} lifts to exactly p^3 solutions of the two congruences (9) and (10) modulo p^{c-1} , since

$$\nabla(2\nu' S'_1 + p^{a+1} S'_2) \equiv 2\nu'(1, 1, -1, -1) \not\equiv 0 \pmod{p}.$$

It follows that (9) and (10) have $p^3 N(p; a+1, c-2)$ solutions, provided of course that $c \geq 2$ for each of the p possible choices of β .

We are therefore able to conclude that

$$N(p; a, c) \leq N_0(p; a, c) + p^4 N(p; a+1, c-2) \leq 2p^{2c} + p^4 N(p; a+1, c-2)$$

for $c \geq 2$, and the lemma then follows by induction on c .

We conclude this section by remarking that in this final inductive argument, we have estimates of the same order of magnitude for both the number of singular solutions and the number of nonsingular solutions. When one tries to generalize the argument to systems of more congruences the singular solutions can dominate the count in an unwelcome way. It is for this reason that Wooley's approach requires a "conditioning" step in general, in order to remove singular solutions at the outset. Fortunately we just manage to avoid this in our situation.

4 Remarks on the Conclusion to the Proof

This final section is intended to shed some light on the argument that leads from Lemma 7 to the theorem.

Suppose one assumes that $J(X) \ll_\varepsilon X^{\theta+\varepsilon}$ for any $\varepsilon > 0$ and that for any positive integers $a \leq b$ one has

$$I_2(X; a, b) \ll_\varepsilon X^{\theta+\varepsilon} p^{\alpha a + \beta b} \quad (11)$$

for some constants α and β , for a suitable range $p \leq X^{\delta(\alpha, \beta)}$, say.

Then Lemma 7 yields

$$I_2(X; a, b) \ll_b X^\theta p^{\alpha' a + \beta' b}$$

for $a \leq b$, with new constants

$$\alpha' = -\frac{10}{3} - \frac{1}{3}\beta, \quad \beta' = \frac{14}{3} + \frac{1}{2}\alpha + \frac{7}{6}\beta - \frac{1}{2}\theta.$$

We can express this by writing

$$\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = \mathbf{c} + M \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

with

$$\mathbf{c} = \begin{pmatrix} -10/3 \\ 14/3 - \theta/2 \end{pmatrix} \quad M = \begin{pmatrix} 0 & -1/3 \\ 1/2 & 7/6 \end{pmatrix}.$$

Starting with $\alpha = \beta = 0$ we can obtain inductively a succession of bounds of the shape (11), with

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix} = \mathbf{c} + M\mathbf{c} + \dots + M^n \mathbf{c}.$$

The matrix M has eigenvalues 1 and $\frac{1}{6}$, and can be diagonalized as PDP^{-1} with

$$P = \begin{pmatrix} -1 & -2 \\ 3 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{6} \end{pmatrix}.$$

It then follows that

$$\begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix} = nP \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} P^{-1} \mathbf{c} + O(1) = \frac{(6-\theta)n}{5} \begin{pmatrix} -1 \\ 3 \end{pmatrix} + O(1)$$

as n tends to infinity. For any starting pair a, b we will have $3b - a \geq 2b \geq 2$. Thus if $\theta > 6$ we will eventually have $\alpha_n a + \beta_n b < -1$, say, for suitably large n .

We therefore obtain

$$I_2(X; a, b) \ll_\varepsilon X^{\theta+\varepsilon} p^{-1}$$

for $p \leq X^\delta$, for some $\delta = \delta_n$ depending on θ . This leads to a contradiction, as in §2.

We therefore see that the crucial feature of Lemma 7 is that it leads to a matrix M having its largest eigenvalue equal to 1. The corresponding eigenvector is $(\alpha, \beta) = (-1, 3)$, and the argument of §2 has therefore been expressed in terms of the linear combination $3b - a$.

References

- [1] J. Bourgain, C. Demeter, and L. Guth, Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three, [arXiv:1512.01565](#).
- [2] K. Ford and T.D. Wooley, On Vinogradov's mean value theorem: strongly diagonal behaviour via efficient congruencing, *Acta Math.*, 213 (2014), 199–236.
- [3] T.D. Wooley, Vinogradov's mean value theorem via efficient congruencing, *Annals of Math.* 175 (2012), 1575–1627.
- [4] T.D. Wooley, Vinogradov's mean value theorem via efficient congruencing, II, *Duke Math. J.* 162 (2013), no. 4, 673–730.
- [5] T.D. Wooley, Multigrade efficient congruencing and Vinogradov's mean value theorem, *Proc. London Math. Soc. (3)*, 111 (2015), no. 3, 519–560.
- [6] T.D. Wooley, Approximating the main conjecture in Vinogradov's mean value theorem, [arXiv:1401.2932](#).
- [7] T.D. Wooley, The cubic case of the main conjecture in Vinogradov's mean value theorem, [arXiv:1401.3150](#).
- [8] T.D. Wooley, Translation invariance, exponential sums, and Waring's problem, *Proceedings of the International Congress of Mathematicians, Seoul, 2014*, pp. 505–529.

Mathematical Institute,
Radcliffe Observatory Quarter
Woodstock Road
Oxford
OX2 6GG
UK

rhb@maths.ox.ac.uk